REMARKS

The Examiner is thanked for the thorough examination of the present application. The Examiner is also thanked for the courtesies extended during the telephonic interview of October 30, 2008, during which the current claim rejections were discussed. The independent claims have been amended to include subject matter similar to that of dependent Claim 9. Dependent Claims 9 and 19 have been cancelled, and dependent Claims 10 and 20 have been amended for consistency. The independent claims have also been amended to remove the recitation of a plurality of different connectors for coupling the cryptographic module to different network devices. New dependent Claims 37 and 38 have been added and include subject matter removed from the independent claims. The patentability of the claims is discussed below.

I. The Claimed Invention

As recited in amended independent Claim 1, for example, the cryptographic device includes a cryptographic module and a communications module removably coupled thereto. The cryptographic module includes a first housing, a user Local Area Network (LAN) interface carried by the first housing, and a cryptographic processor carried by the first housing and coupled to the user LAN interface. Claim 1 has been amended to further recite that the cryptographic module also includes a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. Furthermore, the communications module includes a second housing and a network

wireless LAN interface carried by the second housing coupled to the cryptographic processor and switchable between wireless LAN modes.

Amended independent Claim 11 is directed to a similar cryptographic device, and amended independent Claims 21 and 25 are directed to related methods. Amended independent Claim 29 is directed to a related communications system. Independent Claims 11, 21, 25, and 29 have been amended similar to amended independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected dependent Claims 9 and 19 over Dhir et al. in view of Cheng in further view of Allmond et al., and in further view of Klein. Even a selective combination of the prior art fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing.

Dhir et al. is directed to a programmable integrated circuit, namely a field programmable gate array (FPGA), that can be used to handle different wireless local area network (WLAN) communication specifications. The integrated circuit includes a transceiver coupled to programmable gates, memory coupled to the programmable gates for storing instructions for programming a first portion of the programmable gates with a selected one of a first type of a medium access layer and a second type of a medium access layer. The first type of the medium access layer is different from the second type of medium access layer, though both the first type of the medium access layer and the second

type of the media access layer are compatible with the transceiver. The memory is configured for storing instructions for programming a second portion of the programmable gates as a baseband controller. (See, e.g., Col. 2, lines 14-49 of Dhir et al.).

The Examiner correctly acknowledges that Dhir et al. fails to teach a cryptographic module and a communications module that are removably coupled to one another, a LAN interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices, and a cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner then turned to Cheng for one of these critical deficiencies. Cheng is directed to an add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks. The add-on card includes an access control circuit, volatile and non-volatile memory, a wireless transmission module, and a network connection module. The network connection module has both an antenna for communicating with a wireless network, and a standard network cable port for connecting to a wired network. (See, e.g., paragraphs 0009-0010 of Cheng).

The Examiner still further recognized that even a selective combination of Dhir et al. and Cheng fail to disclose the LAN interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices and the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering

with the first housing. The Examiner turned to Allmond et al. to support one of these deficiencies. More particularly, the Examiner turned to Allmond et al. to support the LAN interface comprising a plurality of different connectors for coupling the cryptographic module to different network devices. However, this recitation has been removed from the independent claims. Accordingly, Applicants understand that the Examiner's rejection of dependent Claims 9 and 19 no longer includes Allmond et al.

The Examiner still further recognized that even a selective combination of Dhir et al. and Cheng fail to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner turned to Klein for this critical deficiency. Klein is directed to data security for digital data storage. More particularly, Klein discloses using a key to encrypt data between a data source and a data storage device.

Applicants submit that the Examiner mischaracterized Klein, as Klein fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner contended that Col. 7, lines 44-45 of Klein disclose a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. Instead, Col. 7, lines 44-45 of Klein disclose, "Tampering with the logic circuit 50 may also result in incorrect key generation." Nowhere else in Klein is tampering mentioned. Indeed, Klein only mentions that tampering with the logic circuit, and not a first housing, may result in incorrect key generation, and not a disablement.

Accordingly, Klein fails to disclose a tamper circuit for disabling the cryptographic processor based upon tampering with said first housing, as recited in the amended independent claims.

Applicants further submit that the Examiner's combination of Dhir et al., Cheng, and Klein is improper, as a person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. and Klein to arrive at the claimed invention. More particularly, Dhir et al. is directed to a programmable logic device for a WLAN. The communications module and the cryptographic module are purposely on a single circuit board (330), as illustrated in Fig. 8 of Dhir et al. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single circuit board.

Moreover, using Cheng as a motivation to modify Dhir et al. would result in arbitrarily dividing the circuitry of Dhir et al. between the antenna 336 and the WLAN transceiver 301, the antenna being outside the circuit board and downstream from both the communications and cryptographic modules. This is because Cheng discloses removably coupling the communications modules to a connector portion, including a physical connector and antenna. Accordingly, even if there was some proper motivation to combine Dhir et al. and Cheng, the claimed invention is not produced because the removable coupling is not between the communications module and the cryptographic module.

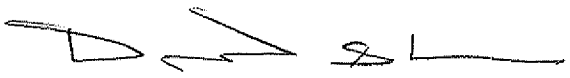
Still further, one of ordinary skill in the art would not turn to the data security system for digital storage to

combine with the programmable integrated circuit from Dhir et al. and the add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks from Cheng. In other words, the Examiner is attempting to combine an FPGA for a wireless LAN with a PCMCIA network add-on card and a system for providing security for digital data stored on data storage media. Applicants submit that the Examiner is merely combining disjoint pieces of the prior art in an attempt to arrive at the claimed invention. Accordingly, it is submitted that the Examiner's combination of references is improper.

III. CONCLUSION

In view of the amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
Attorneys for Applicants